UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/914,258	02/08/2002	Andrew Augustine Wajs	5683P013	2221

21186 7590 10/05/2005

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH
1600 TCF TOWER
121 SOUTH EIGHT STREET
MINNEAPOLIS, MN 55402

EXAMINER	
SZYMANSKI, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/914,258	WAJS ET AL.	
	Examiner	Art Unit	
	Thomas Szymanski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02/08/2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/21/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 have been examined.

Drawings

2. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

4. The applicant is requested to review the specification and update the status of all co-pending applications made mention of, replacing attorney docket numbers with current U.S. application or patent numbers when appropriate. References to U.S.

applications or patents should make it clear as to what the number refers (e.g. U.S. Patent No. #), instead of listing only the number.

5. The disclosure is objected to because of the following informalities: The specification is not arranged properly.

6. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if

the required "Sequence Listing" is not submitted as an electronic document on compact disc).

7. Appropriate correction is required.

8. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claim 4 has been renumbered 1.

Misnumbered claim 5 has been renumbered 2.

Misnumbered claim 6 has been renumbered 3.

The above stated claims have been renumbered in light of the fact that they were included in the document stated as being the preliminary amendment. Another document submitted with the same claims and numbered correctly has been noted but this document was not distinguished as being the preliminary amendment since a proper cover letter and explanation was not included with the file received by the examiner.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Regarding Claims 1-7: The term "high rate" in claims 1, 4, and 6 is a relative term which renders the claim indefinite. The term "high rate" is not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term “high rate” is used by the applicant to describe the frequency at which a first key is changed, but as stated this term lends itself to being indefinite.

12. Regarding Claim 2: The applicant states “wherein instead of an ECM identifying the service key (Pt) an ECM identifying a dummy key (Pd1 or Pd2) to be used identifying a dummy key (Cwi), is sent....”, this language is unclear as to whether the applicant is stating that instead of using and identifying a dummy key (Pd1 or Pd2), the applicant is identifying a dummy key (Cwi) as the incorrect key or they are using the previously stated Pd1 or Pd2 to identify such a key. The claim language is therefore vague and indefinite as it can not be determined to what this language speaks.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

14. Claims 4 -7 are rejected under 35 U.S.C. 102(a) as being anticipated by International application published under the PCT, WO 99/19822 Birdwell et al.

15. Regarding Claim 4: conditional access system comprising a number of subscribers (Fig 1-4, pg 1 lines 17-20, pg 5 lines 15-24)

Each-subscriber having a terminal including a conditional access module and a secure device to store entitlements (Fig 1-4, pg 12 lines 23-24) As shown each client has a secure memory and access module for receiving the content.

A source signal is encrypted using a first key and broadcast for receipt by terminals, first key is changed at a high rate (Fig 1, pg 7 lines 3-10, pg 16 lines 19-20, pg 18 lines 1-25) Birdwell et al teaches changing the keys at a high rate within the suspected group in relation to finding the pirated terminal. Additionally, a first key within the scope of a conditional broadcast system is always changed at a high rate.

Entitlement control messages (ECM's) are sent to the secure devices, comprising the first key encrypted using a service key (pg 5 lines 15-18, Fig 5-7, pg 8 line 20-pg 9 line 2) This system is implemented within a conditional broadcast system as specified, it is well known within such a system that these messages containing the specified encrypted keys are ECM's.

Entitlement management messages (EMM's) are sent to the secure device providing the service key required to decrypt encrypted first keys (Fig 5-6, pg 8 line 20-pg 9 line 2) As stated by Birdwell et al and as denoted above the session keys are encrypted by an authorization key (service key) that is distributed to the client.

A cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate (pg 15 line 21-pg 16 line 15)

Search EMM'S are sent to at least a part of the terminals (pg 16 lines 1-15) As stated the system provides a search message methodology to track down the pirated terminal. Each search EMM of the set comprising a different dummy key (Po) and each EMM being sent to a different part of the terminals (Fig 7, pg 16 lines 9-14) As shown by Birdwell et al within a specified embodiment a different key or dummy key is sent to each involved party.

16. Regarding Claim 5: the terminals are divided into groups, wherein in a first search step the number of search EMM'S of the set of search EMM'S corresponds to the number of groups (Fig 7, pg 16 lines 9-14, pg 17 line 20 – pg 18 line 20)

17. Regarding Claim 6: The source signal or the ECM's are encrypted using a multiple-key or secret-sharing cryptographic algorithm having a plurality of different decrypting keys or shares required for decrypting the encrypted source signal or ECM'S respectively. Plurality of different decrypting keys or shares (Ci;Pi) are sent to at least a part of the terminals such that different terminals or groups of terminals receive different keys or shares according to a predetermined distribution. (pg 15 line 21 – pg 17 line 19, Fig 5-7) Birdwell et al states that different groups of keys are distributed to different sets of terminals. These keys are used within the system to decrypt the control word or first key.

18. Regarding Claim 7: the distribution of the terminals in groups of terminals is varied to trace the cracked secure device (Fig 7 pg 15 line 21 – pg 17 line 19) As it has been shown within the system of Birdwell et al the distribution of the keys within different groups is varied as a process of the implemented algorithm of dissecting such groups by way of the elected group size.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson Multimedia EP 0822720A1, and further in view of Birdwell et al WO 99/19822.

21. Thomson Multimedia teaches a conditional access system that encrypts the first key or control word many different times using a plurality of different keys. (Fig 3a, 3b, Col 6 line 51 – Col 9 line 15)

22. Thomson Multimedia fails to teach tracing pirated terminals through the use of distributed key shares.

23. Birdwell et al discloses a conditional access system for the tracking of pirated terminals by distribution of specific authorization keys to different groups. (pg 15 line 21 – pg 17 line 19)

24. It is desirable within any system to maintain a high level of security and to have the ability to maintain services without the theft of those services occurring and individuals pirating such services through the distribution of sensitive system information. (Birdwell pg 1 line 11 – pg 2 line 19)

25. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the tracking system of Birdwell et al into that of Thomson Multimedia for the advantages of improved system security.

26. Regarding Claim 6: conditional access system comprising a number of subscribers (Birdwell et al Fig 1-4, pg 1 lines 17-20, pg 5 lines 15-24)
Each-subscriber having a terminal including a conditional access module and a secure device to store entitlements (Birdwell et al Fig 1-4, pg 12 lines 23-24) As shown each client has a secure memory and access module for receiving the content.
A source signal is encrypted using a first key and broadcast for receipt by terminals, first key is changed at a high rate (Birdwell et al Fig 1, pg 7 lines 3-10, pg 16 lines 19-20, pg 18 lines 1-25) Birdwell et al teaches changing the keys at a high rate within the suspected group in relation to finding the pirated terminal. Additionally, a first key within the scope of a conditional access system is always changed at a high rate.
Entitlement control messages (ECM's) are sent to the secure devices, comprising the first key encrypted using a service key (Birdwell et al pg 5 lines 15-18, Fig 5-7, pg 8 line 20-pg 9 line 2) This system is implemented within a conditional broadcast system as

specified, it is well known within such a system that these messages containing the specified encrypted keys are ECM's.

Entitlement management messages (EMM's) are sent to the secure device providing the service key required to decrypt encrypted first keys (Birdwell et al Fig 5-6, pg 8 line 20-pg 9 line 2) As stated by Birdwell et al and as denoted above the session keys are encrypted by an authorization key (service key) that is distributed to the client.

27. A cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate (Birdwell et al pg 15 line 21-pg 16 line 15)

28. The source signal or the ECM's are encrypted using a multiple-key or secret-sharing cryptographic algorithm having a plurality of different decrypting keys or shares required for decrypting the encrypted source signal or ECM'S respectively (Thomson Multimedia Fig 3a, 3b) As shown the keys are in the format of a share in the respect that each key is associated by the union of the group to share the decrypting of the data, so thereby providing for such a share of the decrypting.

Plurality of different decrypting keys or shares (Ci;Pi) are sent to at least a part of the terminals such that different terminals or groups of terminals receive different keys or shares according to a predetermined distribution. (Thomson Col 6 line 51 – Col 9 line 15, Birdwell pg 16 lines 9-14) As stated within the Thomson Multimedia document the control words are encrypted with a plurality of different authorization keys and as

provided for by Birdwell et al and Thomson these keys are distributed according to a desired pattern amongst the terminals.

29. Regarding Claim 7: The distribution of the terminals in groups of terminals is varied to trace the cracked secure device (Birdwell et al Fig 7 pg 15 line 21 – pg 17 line 19) As it has been shown within the system of Birdwell et al the distribution of the keys within different groups is varied as a process of the implemented algorithm of dissecting such groups by way of the elected group size.

Allowable Subject Matter

30. Claims 1-3 as best understood would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

31. The following is an examiner's statement of reasons for allowance: PCT application WO 99/19822 to Birdwell et al teaches a conditional access system (Fig 1-4, pg 1 lines 17-20, pg 5 lines 15-24) for the tracking of pirated terminals using a specific traceable authorization key provided to the user prior to the reception of a first key (Fig 5-7, pg 15 line 20 – pg 17 line 20). However, the prior art relied upon fails to teach the use of separate dummy keys in combination with an actual key for tracing such a pirated terminal by the group that contains a certain dummy key and relies upon tracing of the pirated terminal solely on the basis of the one given actual key.

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

33. Inquiries concerning this communication or earlier communications from the examiner should be directed to Thomas M. Szymanski who can be reached at (571) 272-8574. The examiner's normal working schedule is between the hours 8:00am – 4:30pm (EST), Monday – Friday.

34. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

35. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JL

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100